

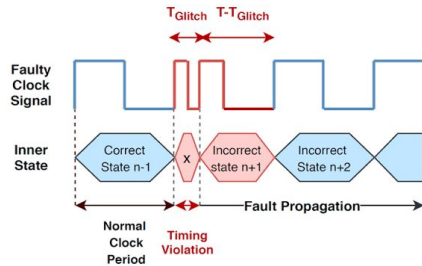
BitCrusher: Affordable, Open Source, Electromagnetic Fault Injection Platform

George Crane, Dean Sullivan
University of New Hampshire
Resilient Architecture Lab

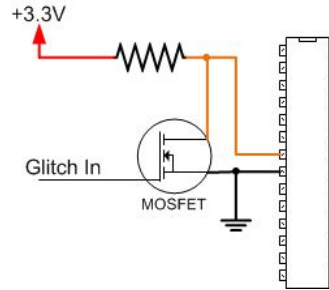
A Brief Introduction to EM Fault Injection

- Fault injection (FI) can be used to bypass security measures in computer systems

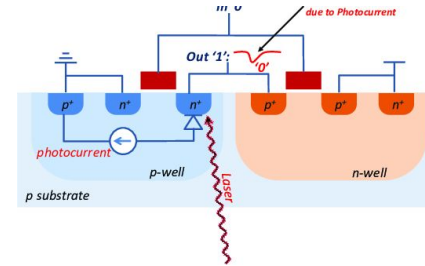
Clock Glitching



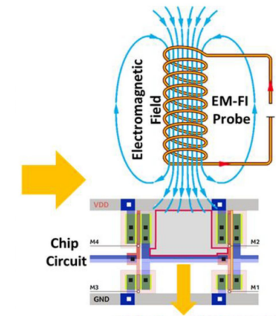
Voltage Glitching



Optical / Laser FI



EMFI



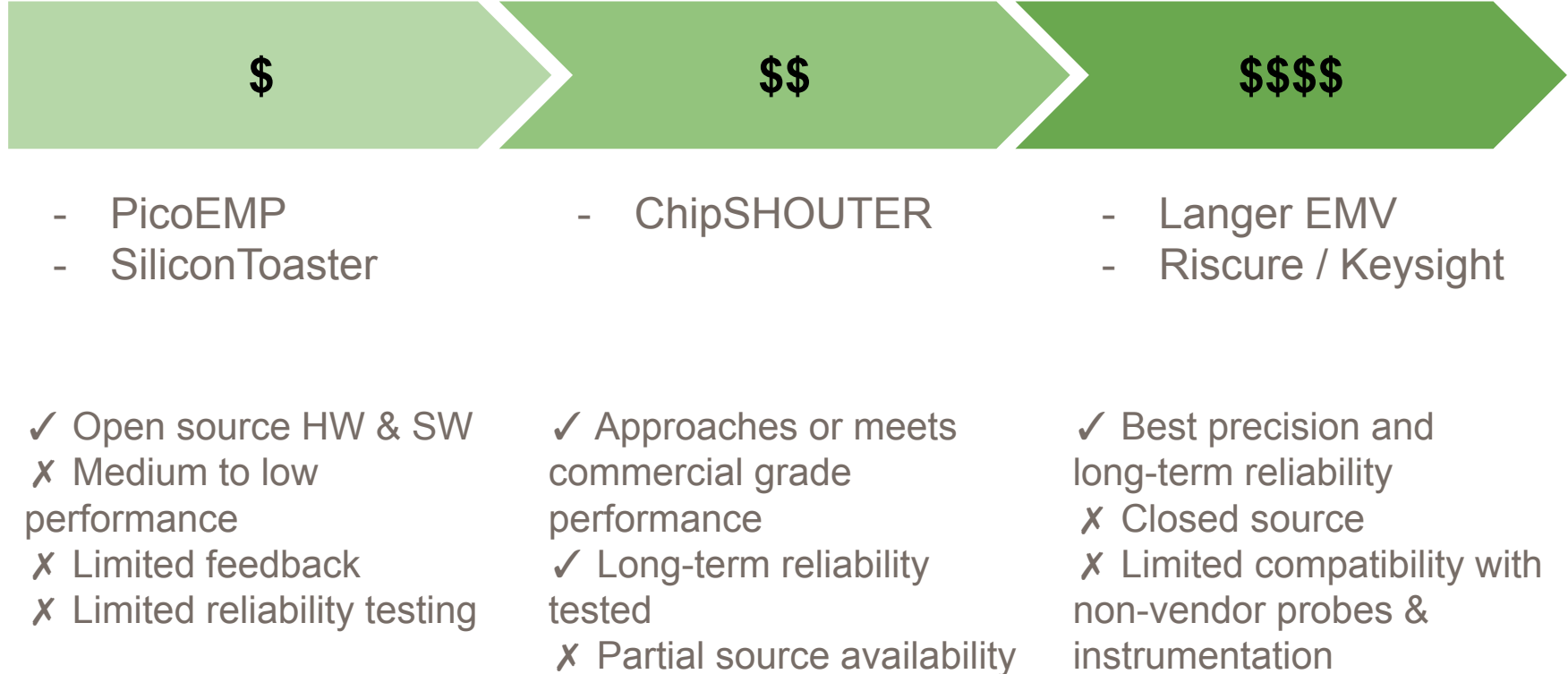
- EMFI offers many benefits over alternative FI techniques
 - Don't need to expose die, unlike optical or current probe techniques
 - Unlike clock or voltage glitching, **specific areas of the chip can be targeted**
 - Inner layers of chip can be faulted** effectively, unlike optical or current probe techniques

A Brief Introduction to EM Fault Injection

What do EMFI researchers need from their instruments?

- High precision **pulse feedback** for **probe characterization** and **comparison to DUT feedback**
- **Integration with existing hardware security instruments** (e.g. ChipWhisperer, positioning systems) for efficient automated experiments
- Enough **design insight** to identify and address instrument limitations

A Brief Introduction to EM Fault Injection



A Brief Introduction to EM Fault Injection

Problem: EMFI Instruments are **very expensive**

I wanted to explore the space

Hard to convince my advisor to give up (tens of) thousands of dollars for me to “explore the space”

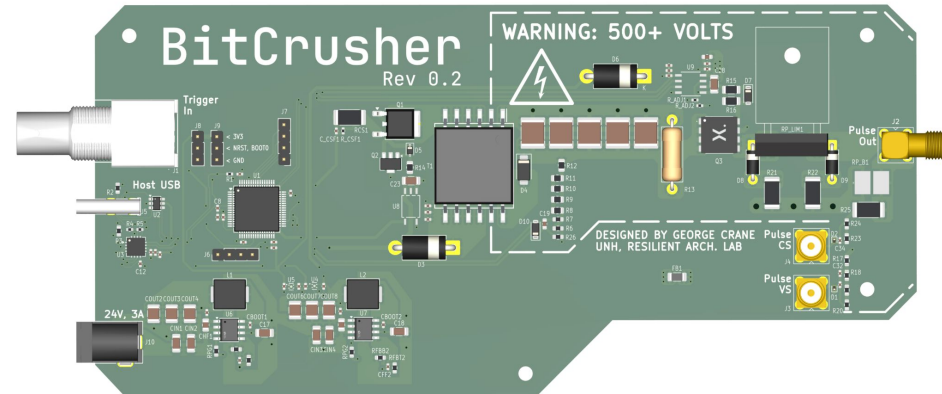
Existing open source options did not have what I needed

I took on this problem as my senior design project

Our Proposed Solution: BitCrusher*

BitCrusher is a **new EMFI research instrument**

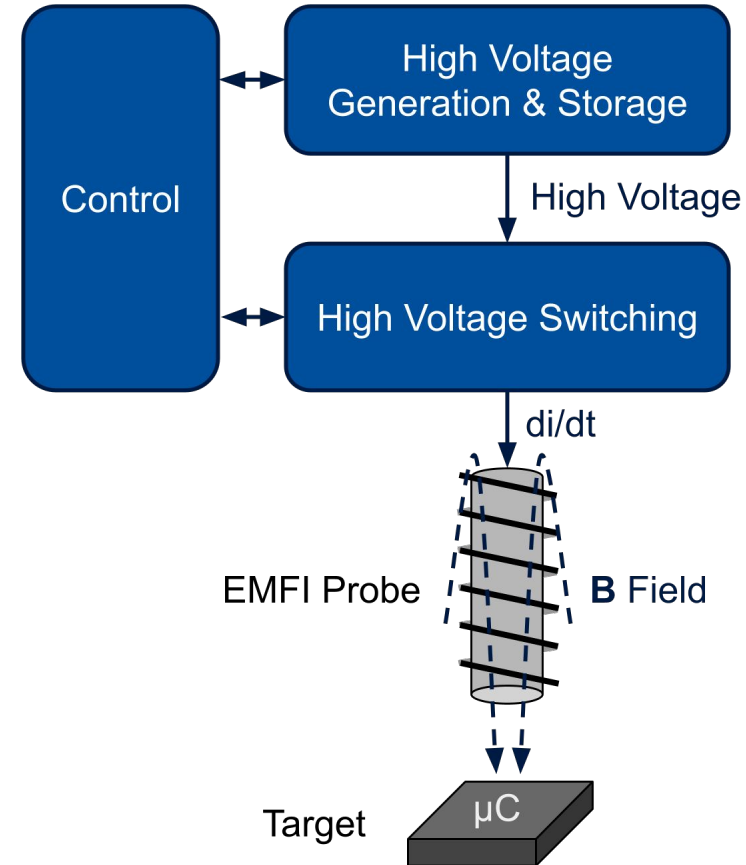
- **Best performance per dollar** of open alternatives, approaching ChipSHOUTER performance
- **Open source hardware, firmware, and software**, designed exclusively with open source or free tools (KiCad, ngspice, julia MTK...)
- USB-C connectivity & python interface for integration with existing tooling
- **~\$100** for PCB, components & assembly, and power supply.



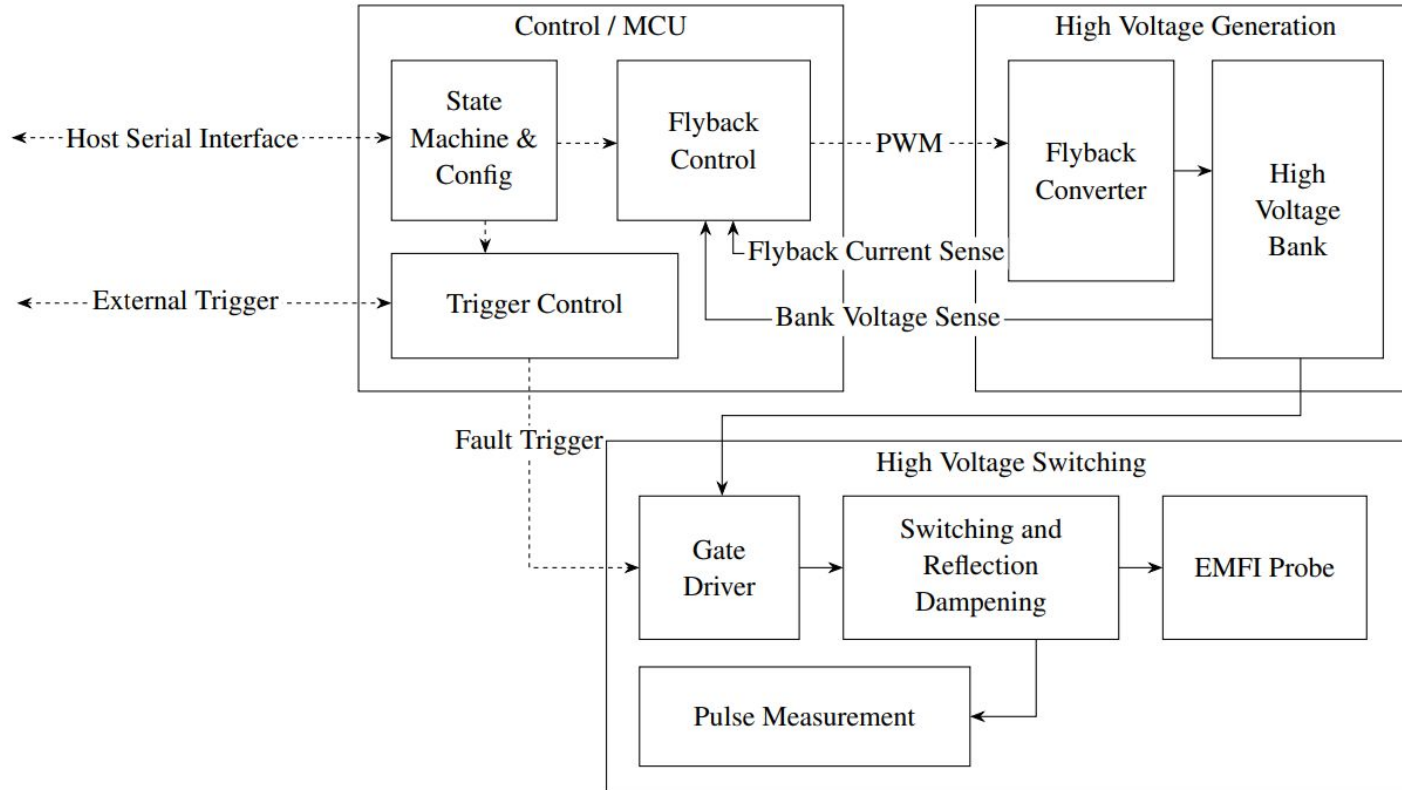
*Yes, like the audio effect

Anatomy of an EMFI platform

- A high voltage is switched over the EMFI probe
- Current through probe induces **B** field
- **B** field through target induces EMF, leading to faults
- Voltage and switching behavior is controlled by user



Anatomy of BitCrusher



Probe Driving Design

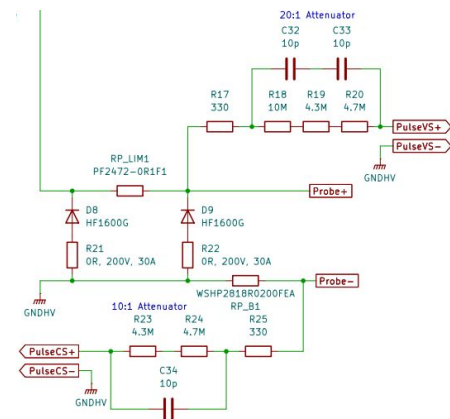
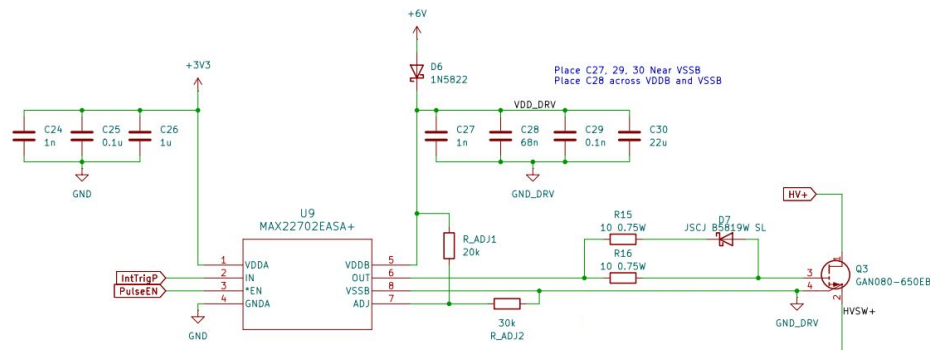
Challenges:

- **Ferrite core EM probes** have effectively **0 DC impedance**. Most impedance from inductance, ferrite core saturation, and near field coupling
- Production **FETs are not characterized for 60A+ nanosecond pulses**
- Probes will create **massive back EMF during turn off**
- Scope probes for **high voltage differential measurement** are **very expensive**

Probe Driving Design

Solutions:

- Design around **simplified linear probe model** with lowest estimate of impedance (**worst case** for current draw and flyback voltage)
- Estimated FET current handling with transient thermal impedance
- **Adjustable flyback compensation circuit**
- **Integrated measurement buffers** to assess probe switching behavior



Host Interface Design

- MCU reset / bootloader control
- Firmware updating
- Trigger configuration
- Voltage generator setpoint
- Temporary & indefinite pulse arming

Interface also enables coordination with other python-controlled instruments (ChipWhisperer, positioning system, PyVISA...)

```
from bitcrusher import Device

def InterfaceListing():
    device = Device() # connect device

    device._flash_firmware("path/to/firmware.bin") # update device firmware

    device.arming_config.voltage = 200
    # configure high voltage generation to 200 volts

    device.arm() # arm (enable FI)

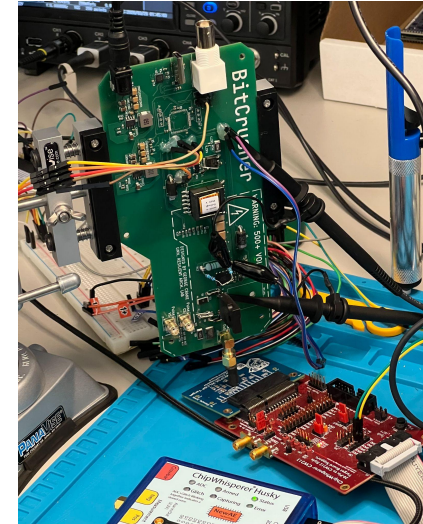
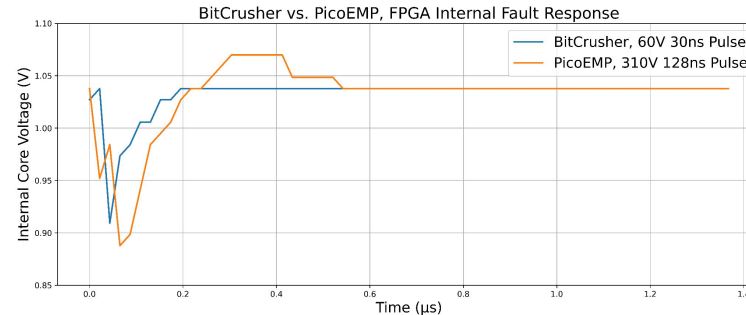
    device.reset() # disarm & reboot
```

Preliminary Assessment of Prototype

Two prototype revisions have been assessed

Basic functionality validated, voltage generator stability issues remain to be fixed in next revision

Repeated injected fault characterization experiment from PicoEMP, improves time resolution and reduces fault overshoot

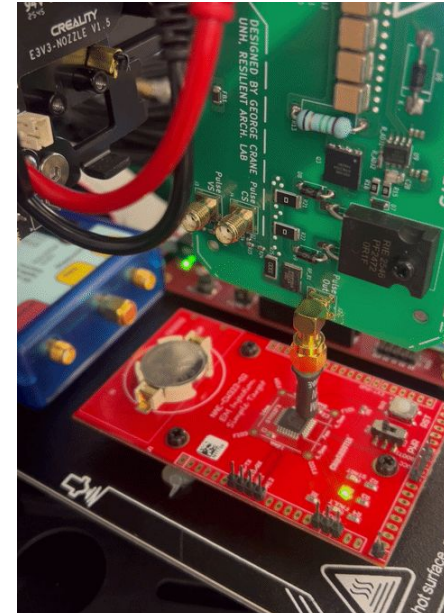
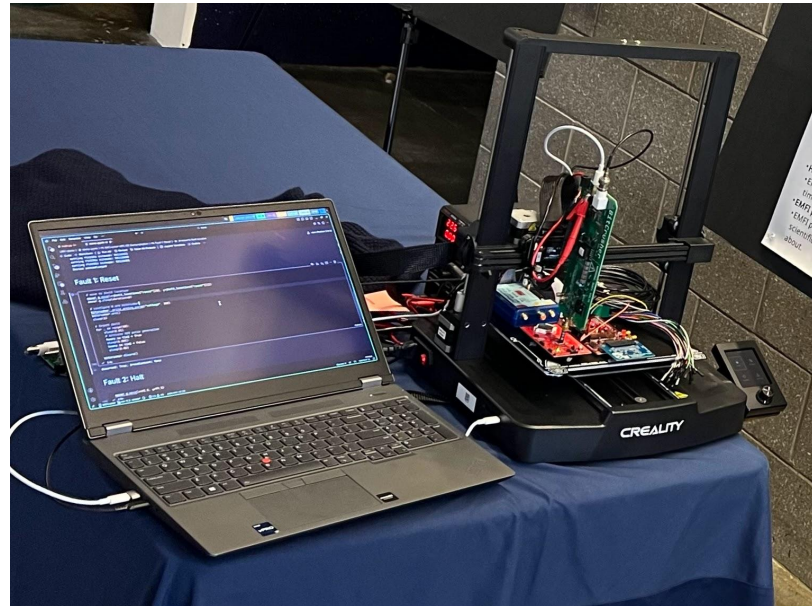


Preliminary Assessment of Prototype

Fault scan over CW322 EMFI test target

Used **3D printer-based positioning system** and a **ChipWhisperer Husky**

Identified **3 unique fault modes**



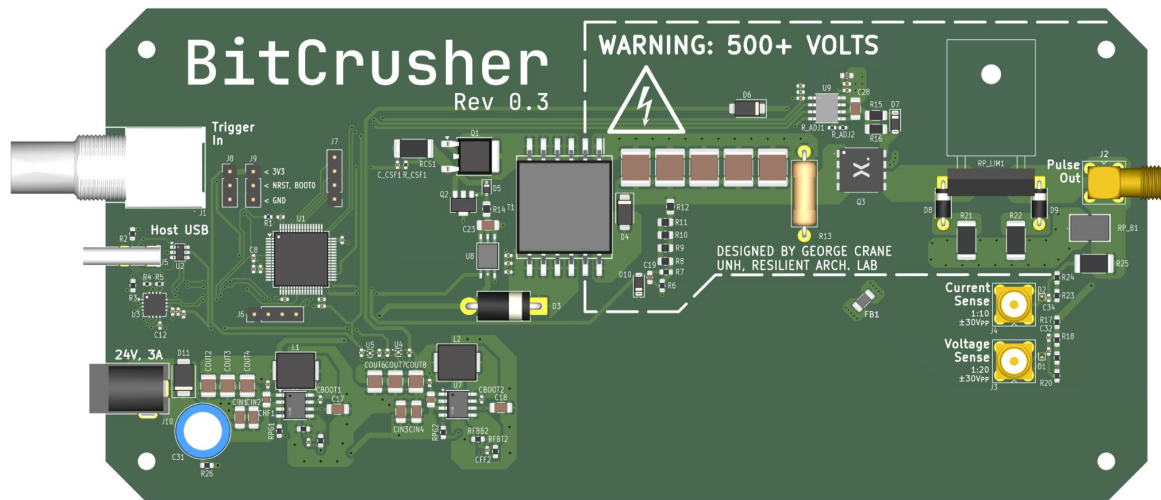
Next Steps & Future Work

Toward probe development & characterization (in progress)

- Voltage generator control system
- Pulse & FET measurement buffers
- FET switching characterization
- Methodology for probe characterization

Toward reliability for long running FI campaigns

- Heat dissipation
- Self-reset / spurious trigger protection



Thank You! Questions?

